RODO

W dniu 25 maja 2018 roku weszły w Polsce w życie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – popularnie zwanego RODO.

RODO

Wprowadzenie RODO jest wynikiem reformy przepisów dotyczących ochrony danych osobowych na obszarze całej Unii Europejskiej.

Zgodnie z Konstytucją RP przepisy RODO stosuje się wprost, a zatem nie wymagają one implementacji do polskiego porządku prawnego (np. w ustawie o ochronie danych osobowych).

RODO (MOTYW 18)

- RODO nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach działalności czysto osobistej lub domowej, czyli bez związku z działalnością zawodową lub handlową.
- Działalność osobista lub domowa może między innymi polegać na korespondencji i przechowywaniu adresów, podtrzymywaniu więzi społecznych oraz działalności internetowej podejmowanej w ramach takiej działalności.
- Niniejsze rozporządzenie ma jednak zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej (np. archiwum w komunikator GG).

Dane osobowe

„dane osobowe” oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”);

Ochrona danych osobowych obejmuje zatem wyłącznie dane osoby fizycznej (człowieka).

Dane osobowe

Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak

- ✓ imię i nazwisko,
- ✓ numer identyfikacyjny (np. NIP lub PESEL)
- ✓ dane o lokalizacji (np. dane GPS lub numer IP urządzenia w sieci)
- ✓ identyfikator internetowy (login)
- ✓ lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Dane osobowe

Forma papierowa - akta osobowe, segregatory, archiwa, umowy z klientami, umowy-zlecenia, faktury

Forma elektroniczna - programy kadrowo-płacowe, bazy klientów, dane na serwerze, pliki na pendrive.

Forma głosowa - centrala telefoniczna

Forma wizyjna - monitoring wizyjny

Dane osobowe

Dla zakwalifikowania danej informacji jako danych osobowych nie ma znaczenia fakt, czy:

- dane osobowe są powszechnie zrozumiałe, wystarczy że może je zrozumieć dany adresat (np. kod genetyczny, czy nr PESEL)
- dane osobowe nie muszą być prawdziwe, co należy rozumieć w ten sposób, że może dotyczyć okoliczności w sposób obiektywny nieistniejących, pod warunkiem jednak, iż może być przypisana do konkretnej, identyfikowalnej osoby fizycznej (np. stan cywilny)

Dane osobowe

Można zatem rozważyć czy w pewnych okolicznościach samo imię i nazwisko to dane pozwalające już na identyfikację osoby fizycznej.

Jeżeli to będzie wyłącznie zestaw „Jan Kowalski” można mieć wątpliwości. Konkretne okoliczności („kontekst”) mogą jednak sprawić, że powyższe dane należy traktować jako dane osobowe.

- ✓ Przykład: na portierni upoważniony do uzyskania kluczy do danego lokalu został wyłącznie „Jan Kowalski”, który np. musi dodatkowo wylegitymować się dowodem tożsamości.
- ✓ Przykład: prezesem spółki wynajmującej cały chroniony budynek jest właśnie „Jan Kowalski”.

Dane osobowe

- ✓Przykład: W metryce danego oprogramowania widoczne są dane w postaci imienia i nazwiska dziecka uczęszczającego do danego przedszkola. Można na podstawie tych danych ustalić, że dziecko o określonym imieniu i nazwisku uczęszcza do danego przedszkola. O ile w takiej sytuacji może budzić wątpliwości fakt, czy mamy tu do czynienia z danymi identyfikującymi konkretną osobę, to już sytuacja gdy w tej samej metryce widnieją jednocześnie dane w postaci imienia, nazwiska i adresu zamieszkania opiekuna tego dziecka nie powinna pozostawiać w tym względzie większych wątpliwości.

Podany wyżej przykład obrazuje sytuację gdy można pośrednio zidentyfikować konkretną osobę fizyczną poprzez zestawienie (powiązanie) danych.

Kategorie danych

Obok danych osobowych „zwykłych” przepisy RODO wyróżniają szczególną kategorię danych osobowych (dane szczególnie wrażliwe). Cechą tych danych jest to, że ich przetwarzanie jest co do zasady prawnie zakazane. Dane te mogą być przetwarzane wyjątkowo tj. wyłącznie w wypadkach enumeratywnie wymienionych w art. 9 i 10 RODO.

Są to następujące dane:

Dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.	Dane osobowe dotyczące wyroków skazujących oraz czynów zabronionych.

Przetwarzanie danych

Wiele osób zastanawia się czy już przetwarza dane osobowe, czy też jeszcze nie ma to miejsca. Wątpliwości winna rozwiać niżej cytowana definicja.

„przetwarzanie” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie”.

Przetwarzanie danych

Przetwarzanie danych

Podkreślić należy, że poszczególne operacje wymienione w definicji „przetwarzania danych” mają charakter przykładowy.

Także tylko dla porządku operacje te zostały przez ustawodawcę opisane w sposób chronologiczny tj. poczynając od „zbierania” danych, aż do ich „usunięcia” lub „zniszczenia”.

Zbiór danych

„zbiór danych” oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie

Pracownicy

- Imię i nazwisko
- Data urodzenia
- Imiona rodziców
- PESEL
- Adres zamieszkania

Klienci

- Imię i nazwisko
- NIP
- Adres siedziby
- Numer rachunku bankowego

Rejestr korespondencji

- Imię i nazwisko
- Adres dla korespondencji

Pseudonimizacja danych

RODO wprowadza definicję pojęcia „pseudonimizacji danych”.

„pseudonimizacja” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Jest to proces, który w odróżnieniu od anonimizacji danych, winien być odwracalny, w tym sensie, że przy zastosowaniu odpowiednich środków możliwe jest ponowne zapoznanie się z danymi osobowymi. Jego zasadniczym przeznaczeniem jest zabezpieczenie danych przed ich ujawnieniem osobom nieuprawnionym.

Administrator danych

„administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

Ze względu na pojemność definicji, administratorem danych może być nawet oddział spółki kapitałowej, o ile samodzielnie ustala cele i sposoby przetwarzania danych.

Każdy pracodawca jest administratorem danych osobowych swoich pracowników.

Podmiot przetwarzający

„podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

Rozróżnienie pomiędzy administratorem danych a podmiotem przetwarzającym powinno być oparte na okolicznościach natury czysto faktycznej, mianowicie na elemencie sprawowania faktycznego władztwa nad przetwarzanymi danymi.

W rezultacie ta sama spółka może jednocześnie pełnić obowiązki:

- administratora - w stosunku do danych przetwarzanych dla własnych celów,
- podmiotu przetwarzającego - w stosunku do danych jej powierzonych np. na podstawie umowy o powierzenie danych

Administrator danych nie może realizować własnych celów przetwarzania w stosunku do powierzonych mu danych osobowych.

Inspektor ochrony danych

Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu /pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Tylko niektóre podmioty są zobowiązane do powołania IOD – najczęściej można go spotkać w sektorze publicznym.

Naruszenie ochrony danych osobowych (incydent)

„naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

Incydent - przykłady

Chronimy się przed incydentami i ich skutkami, takimi jak:

- Pożar, zalanie
- Utrata danych (awarie, brak zasilania, wirusy)
- Świadome skasowanie danych
- Włamanie, kradzież i sprzedaż danych

Incydent - przykłady

Chronimy się przed incydentami i ich skutkami, takimi jak:

- **Wyrzucenie** danych na śmietnik
- **Przekazanie danych** osobie nieupoważnionej
- **Zagubienie** dokumentacji i sprzętu,
- **Przypadkowa** modyfikacja danych
- **Upublicznienie** danych w Internecie
- **Nieuprawniony** dostęp do danych osobowych

Incydent - przykłady

Zasady przetwarzania danych wg RODO

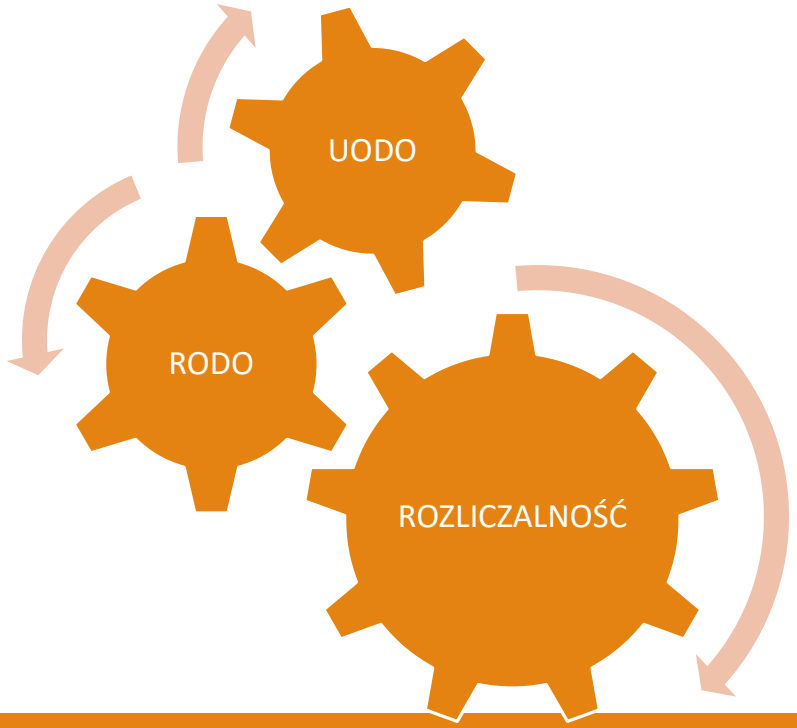
„zgodność z prawem, rzetelność i przejrzystość”	• Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.
„ograniczenie celu”	• Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
„minimalizacja danych”	• Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane

Zasady przetwarzania danych wg RODO – c.d.

„prawidłowość”	• Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.
„ograniczenie przechowywania”	• Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
„integralność i poufność”	• Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Zasady przetwarzania danych wg RODO - c.d.

Administrator jest odpowiedzialny za przestrzeganie przepisów prawa i **musi być w stanie wykazać** ich przestrzeganie („rozliczalność”).



Zasada zgodności przetwarzania z prawem (art. 6 RODO)

Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Zgoda jako podstawa przetwarzania

„zgoda” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

Prawa osoby, której dane dotyczą

Osobom, których dane są przetwarzane przepisy RODO przyznają następujące prawa:

- ✓ prawo dostępu do zbieranych danych osobowych
- ✓ prawo do sprostowania danych
- ✓ prawo do żądania usunięcia danych („prawo do bycia zapomnianym”) ,
- ✓ prawo do ograniczenia przetwarzania,
- ✓ prawo do przenoszenia danych
- ✓ prawo do sprzeciwu
- ✓ prawo do wniesienia skargi do organu nadzorczego

Prawo do usunięcia danych („prawo do bycia zapomnianym”)

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego;

f) dane osobowe zostały zebrane w związku z bezpośrednim oferowaniem dziecku usług społeczeństwa informacyjnego.

Prawo do usunięcia danych („prawo do bycia zapomnianym”)

Prawo do bycia zapomnianym nie ma charakteru bezwzględnego. Osoba, której dane są przetwarzane nie może żądać usunięcia danych w zakresie w jakim przetwarzanie jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;

b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego,

d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że skorzystanie z prawa uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub

e) do ustalenia, dochodzenia lub obrony roszczeń.

Prawa osoby, której dane dotyczą

Administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–22 RODO.

Prawo do wniesienia skargi

Każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza przepisy RODO.

Właściwym organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych.

Wdrożenie odpowiednich środków technicznych i organizacyjnych

Zgodnie z art. 24 i 32 RODO każdy administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać. Takimi środkami są przykładowo:

Środki techniczne	Środki organizacyjne
Szyfrowanie danych	Wdrożona polityka ochrony danych (art. 24 RODO), w tym niezbędne procedury (np. regulamin ochrony danych osobowych)
Pseudonimizacja danych	Szkolenia
Backup danych	Zewnętrzna firma ochroniarska
Uwierzytelniony dostęp do danych	Polityka kluczy
Zabezpieczenia fizyczne i logiczne sieci oraz systemu informatycznego	Zasada czystego biurka
Zabezpieczenia obszaru przetwarzania danych (np. alarm, monitoring wizyjny, zamykane drzwi i kraty w oknach).	Zasada czystego ekranu

Inne wybrane obowiązki administratora

- zawarcie umów o powierzenie danych, w wypadku gdy otrzymuje dane osobowe z zewnątrz lub powierza je na zewnątrz swojej organizacji (art. 28)
- zobowiązanie osób mogących mieć dostęp do danych osobowych do zachowania tajemnicy (art. 5 i 32 RODO),
- należyte upoważnienie każdej osoby mającej dostęp do danych osobowych do ich przetwarzania (art. 29 RODO)
- zgłaszanie naruszenia danych osobowych organowi nadzorczemu bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (art. 33 RODO)
- szacowanie ryzyka - RODO nie odnosi się wprost do procesu zarządzania ryzykiem i nie wskazuje konkretnej metody przeprowadzania oceny w tym zakresie. Każdy podmiot musi dokonywać jej samodzielnie uwzględniając wiele specyficznych dla niego czynników, takich jak: wielkość, struktura organizacyjna, możliwości techniczne czy zakres i rodzaj danych oraz cel ich przetwarzania (stanowisko GIODO).

Inne wybrane obowiązki administratora

W wypadku gdy tego wymaga RODO, administrator może być ponadto zobowiązany do:

- wdrożenia odpowiednich polityk ochrony danych - jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania (art. 24),
- prowadzenia rejestru czynności przetwarzania, w tym prowadzenie takiego rejestru dla danych mu powierzonych – obowiązek ten nie ma jednak zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych (art. 30 RODO).